PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 28 May 2001 (28.05.01)	
International application No. PCT/SE00/01847	**Applicant's or agent's file reference** 55001 PCT si/lt
International filing date (day/month/year) 22 September 2000 (22.09.00)	**Priority date** (day/month/year) 22 September 1999 (22.09.99)
Applicant ALMESÅKER, Marieanne et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

12 March 2001 (12.03.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Nestor Santesso
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

To:

BERGLUND, Stefan
Bjerkéns Patentbyrå KB
Östermalmsgatan 58
S-114 50 Stockholm
SUÈDE

INFORMATION CONCERNING ELECTED OFFICES NOTIFIED OF THEIR ELECTION

(PCT Rule 61.3)

Date of mailing (day/month/year) 28 May 2001 (28.05.01)	
Applicant's or agent's file reference 55001 PCT si/lt	**IMPORTANT INFORMATION**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/SE00/01847	22 September 2000 (22.09.00)	22 September 1999 (22.09.99)

Applicant
SAAB AB et al

1. The applicant is hereby informed that the International Bureau has, according to Article 31(7), notified each of the following Offices of its election:

   EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
   National :AU,BG,CA,CN,CZ,DE,IL,JP,KP,KR,MN,NO,NZ,PL,RO,RU,SE,SK,US

2. The following Offices have waived the requirement for the notification of their election; the notification will be sent to them by the International Bureau only upon their request:

   AP :GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW
   EA :AM,AZ,BY,KG,KZ,MD,RU,TJ,TM
   OA :BF,BJ,CF,CG,CI,CM,GA,GN,GW,ML,MR,NE,SN,TD,TG
   National :AE,AG,AL,AM,AT,AZ,BA,BB,BR,BY,BZ,CH,CR,CU,DK,DM,DZ,EE,ES,FI,GB,
   GD,GE,GH,GM,HR,HU,ID,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MW,
   MX,MZ,PT,SD,SG,SI,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

3. The applicant is reminded that he must enter the "national phase" **before the expiration of 30 months from the priority date** before each of the Offices listed above. This must be done by paying the national fee(s) and furnishing , if prescribed, a translation of the international application (Article 39(1)(a)), as well as, where applicable, by furnishing a translation of any annexes of the international preliminary examination report (Article 36(3)(b) and Rule 74.1).

   Some offices have fixed time limits expiring later than the above-mentioned time limit. For detailed information about the applicable time limits and the acts to be performed upon entry into the national phase before a particular Office, see Volume II of the PCT Applicant's Guide.

   The entry into the European regional phase is postponed **until 31 months from the priority date** for all States designated for the purposes of obtaining a European patent.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:
Nestor Santesso

Telephone No. (41-22) 338.83.38

PATENT COOPERATION TREAT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
55001 PCT si/AK		
International application No.	International filing date *(day month year)*	Priority date *(day month year)*
PCT/SE00/01847	22.09.2000	22.09.1999
International Patent Classification (IPC) or national classification and IPC7		
G06F 9/445, G06F 11/00, G06F 11/30		
Applicant		
SAAB AB et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12.03.2001	17.12.2001
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Telex 17978 PATOREG-S Facsimile No. 08-667 72 88	Authorized officer Pär Heimdal/LR Telephone No. 08-782 25 00

Form PCT/IPEA/409 (cover sheet) (January 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/SE00/01847

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
  - pages 1-11, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____
- ☒ the claims:
  - pages _____, as originally filed
  - pages _____, as amended (together with any statement) under article 19
  - pages _____, filed with the demand
  - pages 12-15, filed with the letter of 26.10.2001
- ☒ the drawings:
  - pages 1/1, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
  - pages _____, as originally filed
  - pages _____, filed with the demand
  - pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language english which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☒ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages _____
   - ☐ the claims, Nos. _____
   - ☐ the drawings, sheet/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2 (c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-15	YES
	Claims		NO
Inventive step (IS)	Claims	1-15	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-15	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

CITATIONS
The examination process has revealed the following documents, which represent the general state of the art:

D1: WO 99 08 186 A1
D2: US 5 247 659 A
D3: US 5 432 927 A
D4: US 4 491 914 A

STATEMENT
The document D1 discloses a method and apparatus for providing fault-tolerance for in-circuit programming systems. The invention operates by storing a minimal set of code to initialise the in-circuit programming process in a protected memory (107) so that if the programming process fails, the process can be restarted from the protected memory, see abstract.

The computer device known from D1, comprises processor means, an ordinary memory unit connected to the processor means and a supervisory unit, see figure 1 and page 6, line 11-17.

The computer device known from D1 also includes a further memory unit that is arranged to comprise system instructions, wherein the computer device is arranged such that the processor means, at a restart is connected to the further memory unit and reads and executes instructions that are stored in the same, while the ordinary memory unit is disconnected from the processor means, see page 7, line 8-20.

The further memory unit (ROM) mentioned in D1 and the ordinary memory unit (Flash) constitute two different, physically separate, memories, see page 7, line 17-20 and claim 24. The

.../...

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: V

memory units are non-volatile memories. In a preferred embodiment, the two memory units constitute two parts of physically the same memory, but with different memory addresses, see claim 22. The further memory is write protected, when the computer is operative, see claim 23.

The supervisory unit in D1 is arranged to generate a signal in dependence of a timer in such a manner that said restart signal is generated if no trigger-signal signal that sets the timer to zero is received within a predetermined time interval, see page 8, line 5-13.

The memory safety circuit known from D1 is arranged to stop the reading from the ordinary memory unit and to connect for reading from said further memory unit when the restart signal is given, see page 9, line 2-11. The further memory unit is arranged to include system instructions with a high degree of functional security, see page 3, line 19-23.

However, the claimed invention according to claims 1-15 is considered to deviate from the invention previously described in D1 in several ways. The invention in D1 concerns a computer arrangement with a security function adapted to be used for in-circuit programming systems. The mini-boot-code (107) is used for reboot only when in-circuit programming is carried out. According to the invention, restart is always performed from a further memory unit, while the ordinary memory unit is disconnected.

Accordingly, the invention defined in claims 1-15 is novel and is considered to involve an inventive step. The invention is industrially applicable.

Also document D2 discloses a computer device with a security function, see abstract.

On power-up or system restart, the non-volatile store is tested. If the test is satisfactory, the bootstrap program is loaded from the normal load path. If not, the undefined bootstrap procedure may be entered.

The invention described in D3 includes processor means, an ordinary memory unit connected to the processor means, auxiliary memory means and a supervisory unit, see claim 1.

The auxiliary memory means known from D3 is arranged to

.../...

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: suppl.1

comprise system instructions, wherein the computer device is arranged such that the processor means, at a restart is connected to the further memory unit and reads and executes instructions that are stored in the same, while the ordinary memory unit is disconnected from the processor means, see claim 1.

Document D4 presents yet another computer device with a security function, see abstract. The invention presented in D4 comprises two memories, see figure 3.

However, none of the cited documents D2-D4, or any relevant combination of them reveals a computer with a safety function as defined by claims 1-15.

Therefore the invention according to claims 1-15 is considered to meet the criteria of novelty, inventive step and industrial applicability.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22220 A1

(51) International Patent Classification[7]: G06F 9/445, 11/00, 11/30

(21) International Application Number: PCT/SE00/01847

(22) International Filing Date:
22 September 2000 (22.09.2000)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
9903422-5 22 September 1999 (22.09.1999) SE

(71) Applicant *(for all designated States except US)*: **SAAB AB** [SE/SE]; S-581 88 Linköping (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ALMESÅKER, Marieanne** [SE/SE]; Ekkällegatan 3, S-582 30 Linköping (SE). **NYSTRÖM, Bengt** [SE/SE]; Dillstigen 6, S-589 23 Linköping (SE).

(74) Agents: **BERGLUND, Stefan** et al.; Bjerkéns Patentbyrå KB, Östermalmsgatan 58, S-114 50 Stockholm (SE).

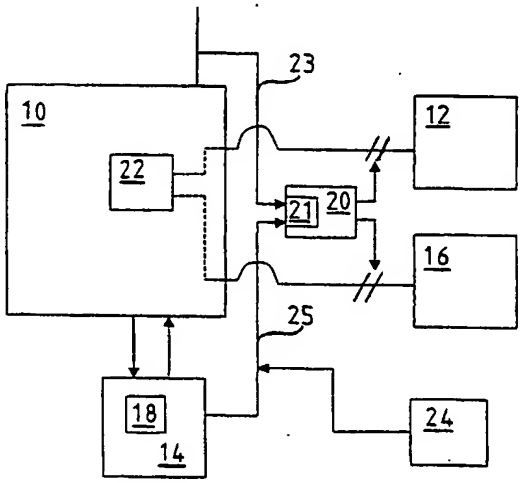
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A COMPUTER DEVICE WITH A SAFETY FUNCTION



(57) Abstract: The invention concerns a computer device with a safety function in order to avoid non-necessary disconnection of the computer device. The computer device comprises processor means (10), an ordinary member unit (12), a supervisory unit (14) and a further member unit (16). The computer device is arranged such that the processor means (10) at a restart generated by a restart signal, is connected to the further memory unit (16) and reads and executes the instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10).

WO 01/22220 A1

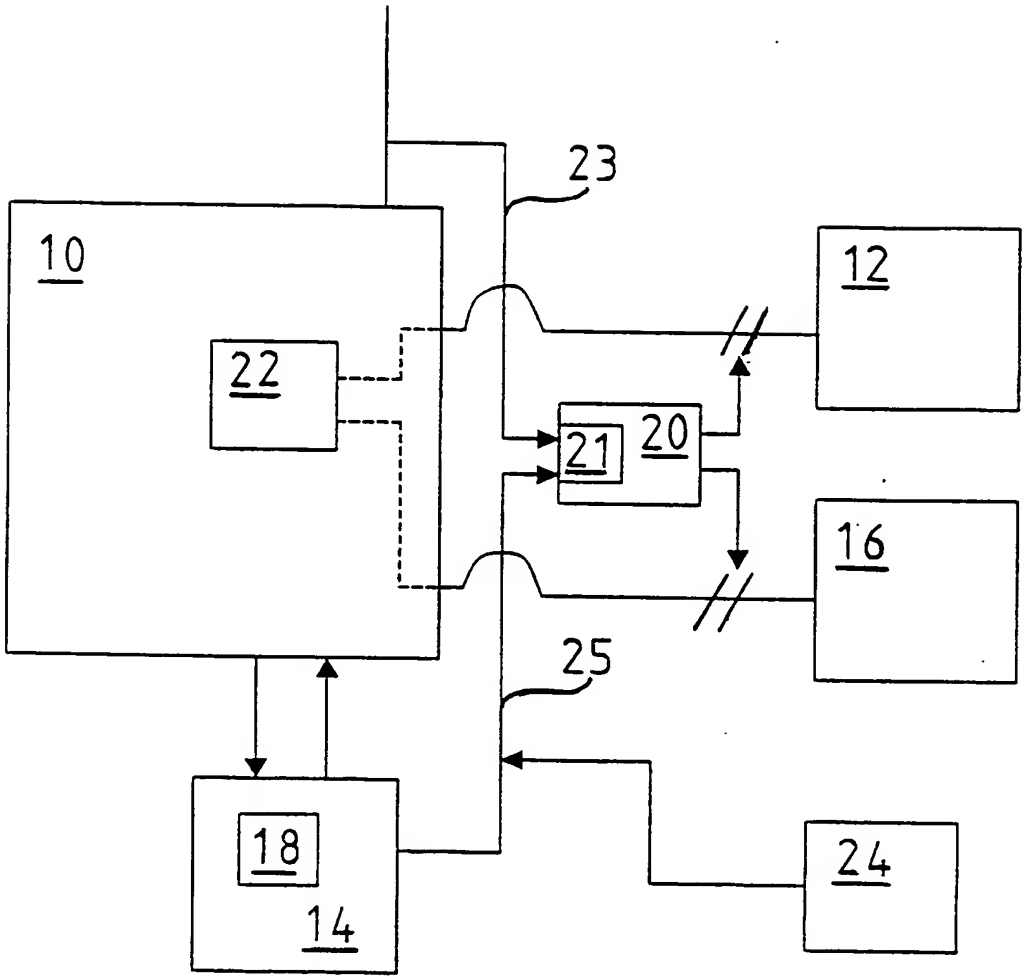


FIG. 1

A COMPUTER DEVICE WITH A SAFETY FUNCTION

BACKGROUND OF THE INVENTION AND PRIOR ART

The present invention concerns a computer device with a safety function for avoiding non-necessary disconnection of the computer device, comprising processor means, an ordinary memory unit connected to said processor means and arranged to comprise at least one program that is executed by the processor means, a supervisory unit that supervises the function of the computer device and that is arranged to, in case an error occurs, send a restart signal or a stop signal to the processor means.

Such computer devices are already known. The supervisory unit may for instance constitute a so-called "watchdog timer". US-A-4 763 296 describes the function of such a watchdog timer. Such a device thus has a timer that continuously is in operation when the computer device is used. If the timer reaches a predetermined value, i.e. if a predetermined time has elapsed, the watchdog timer generates a restart signal that causes a restart (reset) of the computer device. During normal use, the timer is set to zero at regular intervals by the normal program execution by the processor. In case an error occurs, for example if the computer executes an infinite subroutine, the timer will not be set to zero and the watchdog timer thus causes a restart of the system.

Also other kinds of computer devices with safety functions are already known. EP-A-481 508 thus describes a device that comprises a backup memory. When the current supply to the computer device is shut off, the status of the central processor and the content in a main memory are transferred to said backup memory. When then the computer device is started once again by

again connecting the current supply, that which is stored in the backup memory will be restored.

EP-A-265 366 describes a computer device that comprises a primary memory and a backup memory. Switching from the primary memory to the backup memory is done by means of a "Backup Control System Transfer Mechanism". This mechanism is relatively complicated. At the generation of a power-on-reset signal, said mechanism secures that restart is done from the primary memory (see column 6, lines 21-28).

There exists a need to improve the safety function of a computer device. There is thus a need of in a safe manner restarting the computer device when an error has been detected. Such an error that may cause errors in the operation of the computer is for example memory errors that may occur in the memory where programs that are executed in the computer device are stored. An error may also be caused by the software that is stored in the memory of the computer device. Such errors may for example occur when new software is used that has not been completely tested. Furthermore, there exists a need to secure the function of the computer device by relatively simple means. A further problem is to secure at least certain basic functions of the computer device when different errors occur.

SUMMARY OF THE INVENTION

The purpose of the present invention is to achieve a computer device with a reliable safety function that, furthermore, is achieved by relatively simple means.

This purpose is achieved by the initially defined computer device that is characterised by a further memory unit that is arranged to comprise at least some basic system instructions, wherein the computer device is arranged such that the processor means, at a restart generated by said restart signal from the supervisory unit, is connected to the further memory unit and reads and executes

instructions that are stored in the same, while the ordinary memory unit is disconnected from the processor means.

By the fact that the processor means is connected to the further memory unit when a restart signal has been generated by the supervisory unit, it is avoided that possible errors that are present in the instructions that are stored in the ordinary memory unit are transferred to the processor means. A safer function of the computer device after that a restart signal has been generated in response to a detected error is thereby achieved. In this context it should be noted that when in the claims and in the description it is mentioned that a memory unit is connected to or is disconnected from the processor means, it is thereby not necessarily meant that the disconnection is done by physically breaking the connection between the processor means and the memory unit in question. The concepts connect to and disconnect thus comprise two possibilities: physical switching by breaking the connection, and the connection to and the disconnection from at a program level.

It should be noted that by the concept "system instructions" is in this application preferably, but not necessarily, meant programs that control a system or a part of a system that is controlled by the computer device, i.e. the concept "system instructions" concerns application instructions.

According to an embodiment of the invention, the ordinary memory unit and the further memory unit constitute two different, physically separate, memories. By this feature an increased security is achieved since the ordinary memory unit is arranged as a separate memory that is completely disconnected from the processor means at a restart.

According to an alternative embodiment of the invention, the ordinary memory unit and the further memory unit constitute two parts of physically the same memory, but with different memory addresses. Through this construction fewer memory components

are needed since the further memory unit is stored as a special part of the memory where also the ordinary memory unit is included.

According to a further embodiment of the invention, said supervisory unit is arranged to generate a signal in dependence of a timer in such a manner that said restart signal is generated if no trigger signal that sets the timer to zero is received within a predetermined time interval. The supervisory unit may in this case thus constitute a so-called watchdog timer (WDT). Such a WDT often forms part of computer devices. Such a well functioning and already existing WDT may thus be used as a supervisory unit in the device according to the present invention. It should however be noted that also other kinds of supervisory units than a WDT may be used in the computer device according to the invention.

According to still another embodiment of the invention, the computer device comprises a memory safety circuit that is arranged to stop the reading from the ordinary memory unit and to connect for reading from said further memory unit when both said restart signal and a signal indicating applied supply voltage is the case. Such a memory safety circuit is a relatively simple and well functioning circuit that controls that switching from the ordinary to the further memory unit takes place. Furthermore, this memory safety circuit secures that such a switching only occurs if supply voltage to the computer device is present.

According to a further embodiment of the invention, said further memory unit is arranged such that it comprises basic system instructions with a high degree of reliability. The further memory unit may hereby be arranged to comprise system instructions that have already been thoroughly tested and that therefore have a high functional reliability. The further memory unit may hereby also be provided with the basic system instructions for the computer device while non-necessary system instructions have been excluded from said further memory unit.

According to still another embodiment of the invention, said further memory unit is arranged such that it comprises system instructions with a degree of reliability that is higher than the degree of reliability that is the case in the ordinary memory unit. The ordinary memory unit may thus comprises system instructions that have not been so thoroughly tested in the computer device. The further memory unit may thereby comprise the basic system instructions that have already been shown to have a high reliability. Within the frame of the invention is of course also the possibility that the ordinary memory unit and the further memory unit comprise system instructions with the same degree of reliability.

According to a further embodiment of the invention, at least said further memory unit is a non-volatile memory. This fact contributes to an increased functional reliability of the computer device.

According to still another embodiment of the invention, said processor means comprises a working memory that is arranged such that at a restart of the computer device this working memory is reset before reading from said further memory unit is started. By this feature is secured that instructions that may comprise errors and that originate from the ordinary memory unit do not maintain in the working memory before reading from the further memory unit is started.

According to a further embodiment of the invention, said further memory unit is arranged to be write protected at least when the computer device is in operation. This fact contributes to further safety since the content in this further memory unit is protected and may not be modified when the computer device is in operation.

According to still another embodiment of the invention, the computer device is arranged such that if said restart signal has been generated a predetermined number of times, then, in case an error occurs again, said stop signal is generated. This means that the supervisory unit generates a predetermined number of restart signals. If it happens that an error is the case even after that a

predetermined number of restart attempts have been made, the computer device is stopped.

According to still another embodiment of the invention, the computer device comprises a switching member for manually generating said restart signal. This means that in addition to automatic generation of a restart signal by the supervisory unit, also a manual restart signal may be generated by an operator. An operator may thus order that a restart from the further memory unit is to take place.

A further embodiment of the invention is clear from claim 13. This embodiment may also be combined with the features of one or more of the claims 2-12.

The purpose of the invention is also achieved by a method according to claim 14. This method has advantages corresponding to those described in connection with the device. The method according to claim 14 may also be combined with features corresponding to those defined in one or more of the claims 2-12.

A preferred use of the computer device is to use it to control a system that is included in different vehicles, for example in aircrafts. An aircraft has many different functions that are controlled by a computer device. It is important that these functions function and that unnecessary disconnection of the computer device or of its operation concerning some application is avoided. This aim is achieved by a use according to claim 15.

SHORT DESCRIPTION OF THE DRAWING

The present invention will now be explained by means of a described embodiment, which constitutes an example of the invention, and with reference to the annexed drawing.

Fig 1 shows schematically a block diagram of an embodiment of the invention.

DETAILED DESCRIPTION OF AN EMBODIMENT OF THE INVENTION

Fig 1 shows a block diagram of an embodiment of the invention. The computer device comprises a processor means 10. With this processor means 10 is meant not only the central processor unit (CPU) of the computer device but also other central parts of the computer device such as for example the working memory 22. The computer device also comprises an ordinary memory unit 12. This ordinary memory unit 12 may for example constitute some kind of PROM, for example UVPROM, EEPROM or the like. When the computer device first is started, the processor means 10 is connected to the ordinary memory unit 12. This ordinary memory unit 12 is thus arranged to comprise the instructions that control the operation of the computer device. The computer device also comprises a supervisory unit 14. The supervisory unit 14 supervises the function of the computer device and is arranged to generate a restart signal or a stop signal to the processor means 10 if the supervisory unit 14 detects an error. The supervisory unit 14 may for example constitute a so-called watchdog timer (WDT). Such a WDT 14 generates a signal that depends on a timer 18. A restart signal is thereby generated if the WDT 14 within a predetermined time interval does not receive a trigger-signal that sets the timer 18 to zero. In order to have a high reliability, the WDT 14 comprises suitably its own timer 18. It is however possible that the timer function of the WDT 14 is controlled by the same clock that is included in the processor means 10.

The computer device also comprises a further memory unit 16. This further memory unit 16 is arranged to comprise at least some basic system instructions. The further memory unit 16 may constitute a memory that is physically separated from the ordinary memory unit 12. It is also possible that the ordinary memory unit 12 and the further memory unit 16 constitute two parts of physically the same memory. In order to further increase the reliability in case a memory error should occur, the ordinary memory unit 12 and the further

memory unit 16 may constitute physically separate memories of different kinds, for example from different manufacturers. The further memory unit suitably constitutes some kind of PROM, for example UVPROM or EEPROM.

The computer device also comprises a memory safety circuit 20. This memory safety circuit 20 may form a part of the processor means 10. In the shown embodiment, the memory safety circuit 20 however constitutes a separate circuit. The memory safety circuit 20 comprises an AND-gate 21. The memory safety circuit 20 controls which of the ordinary memory unit 12 and the further memory unit 16 that is to be connected to the processor means 10. This control may either be formed by opening or closing the electric connection between the respective memory unit 12, 16 and the processor means 10 or also be formed by a control on a program level of these connections. It is also possible that the control is done by a combination of software instructions and physically opening or closing. One input of the AND-gate is connected to a line 23 that indicates that a supply voltage is present. The other input of the AND-gate 21 is connected to a line 25 that is connected to the WDT 14. Via this line 25, a restart signal generated by the WDT 14 is lead to the AND-gate 21 and thereby to the memory safety circuit 20.

The computer device also comprises a switching member 24 for manually generating a restart signal. This switching member 24 may suitably be connected to the input of the AND-gate that is also connected to the WDT 14.

The WDT 14 thus supervises the function of the computer device. When the computer device functions normally, the WDT 14 receives at regular intervals a trigger-signal from the processor means 10. This trigger-signal sets the timer 18 to zero. The WDT 14 does thereby not generate any restart signal to the line 25. If, however, an error occurs such that the WDT 14 does not receive any trigger-signal from the processor means 10 within a predetermined time interval, the WDT 14 generates a restart signal. This restart signal

is thus lead to one of the inputs of the AND-gate 21. When the AND-gate 21 receives such a restart signal, and if at the same time the other input of the AND-gate 21 detects that a supply voltage is the case, the memory safety circuit 20 controls that the ordinary memory unit 12 is disconnected from the processor means 10 and that the further memory unit 16 is connected to the processor means 10. Also the processor means 10 receives a signal, suitably from the WDT 14, that a restart is to be performed. The working memory 22 of the processor means 10 is thereby reset, whereafter reading from the further memory unit 16 takes place. The reading is thereby done to predetermined addresses of the working memory 22. The processor means 10 thus reads and executes the instructions that are stored in the further memory unit 16.

It is conceivable that a restart attempt fails and that the WDT 14 thus generates a new restart signal. If again an error is detected, further restart signals may be generated by the WDT 14. The computer device is thereby suitably arranged such that when a predetermined number of restart attempts have been made, the restart attempts are stopped. A warning function may thereby be generated by the computer device and the latest information concerning the status of the processor means 10 and the memory units 12, 16 may be registered for later analysis. The computer device is suitably arranged such that the restart attempts are stopped after for example one to four restart attempts, preferably after two restart attempts. The computer device may thereby be arranged such that the restart attempts are stopped if said predetermined number of restart attempts have been performed within a predetermined time interval.

In order to increase the safety, the further memory unit 16 is suitably arranged such that it is write protected when the computer device is in operation. Furthermore, suitably the ordinary memory unit 12 as well as the further memory unit 16 constitute non-volatile memories.

The further memory unit 16 is suitably arranged such that it comprises basic system instructions with a high degree of reliability. The further memory unit 16 may thereby comprise primary and well-tested system functions. Suitably, the further memory unit 16 is arranged such that it thereby comprises system instructions with a higher degree of reliability than the system instructions that are present in the ordinary memory unit 12. By the expression "degree of reliability" may hereby for example be meant the software safety levels that are defined according to RTCA-standard document NO.RTCA/DO-178B.

The computer device according to the invention may preferably be arranged to secure the normal function of the computer device under the execution of an application program even when an error occurs that otherwise would lead to a disconnection and a shut-off of the computer device, or at least to the interruption of the execution of the application program in question. The ordinary memory unit 12 thus comprises an application program that is executed by the processor means 10. In case an error occurs in the execution of at least said application program, the processor means 10 is connected to the further memory unit 16 that is arranged to comprise at least some basic, already used and safe application instructions. The computer device is thus arranged such that the execution of the application that is controlled by the application program may continue on the basis of the application instructions that are retrieved from the further memory unit.

According to a method according to the invention, if an error occurs, a connection to the further memory unit 16 that comprises at least some basic application instructions takes place. The execution of the application that is controlled by an application program may thereby continue on the basis of the application instructions that are retrieved from the further memory unit and that are read in a normal and traditional manner into the processor means 10 with a normal reset of the working memory 22.

The computer device according to the invention may also advantageously be used to control a system that is included in an aircraft.

The present invention is not limited to the shown embodiment but may be varied and modified within the scope of the following claims.

Claims

1. A computer device with a safety function for avoiding non necessary disconnection of the computer device, comprising

processor means (10),

an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least one program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs, send a restart signal or a stop signal to the processor means (10),

characterised by

a further memory unit (16) that is arranged to comprise at least some basic system instructions, wherein the computer device is arranged such that the processor means (10), at a restart generated by said restart signal from the supervisory unit (14), is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10).

2. A computer device according to claim 1, wherein the ordinary memory unit (12) and the further memory unit (16) constitute two different, physically separate, memories.

3. A computer device according to claim 1, wherein the ordinary memory unit (12) and the further memory unit (16) constitute two parts of physically the same memory, but with different memory addresses.

4. A computer device according to any of the preceding claims, wherein said supervisory unit (14) is arranged to generate a signal in dependence of a timer (18) in such a manner that said restart signal is generated if no trigger-signal signal that sets the timer (18) to zero is received within a predetermined time interval.

5. A computer device according to any of the preceding claims, comprising a memory safety circuit (20) that is arranged to stop the

reading from the ordinary memory unit (12) and to connect for reading from said further memory unit (16) when both said restart signal and a signal indicating applied supply voltage is the case.

6. A computer device according to any of the preceding claims, wherein said further memory unit (16) is arranged such that it comprises basic system instructions with a high degree of reliability.

7. A computer device according to claim 6, wherein said further memory unit (16) is arranged such that it comprises system instructions with a degree of reliability that is higher than the degree of reliability that is the case in the ordinary memory unit (12).

8. A computer device according to any of the preceding claims, wherein at least said further memory unit (16) is a non-volatile memory.

9. A computer device according to any of the preceding claims, wherein said processor means (10) comprises a working memory (22) that is arranged such that at a restart of the computer device this working memory (22) is reset before reading from said further memory unit (16) is started.

10. A computer device according to any of the preceding claims, wherein said further memory unit (16) is arranged to be write protected at least when the computer device is in operation.

11. A computer device according to any of the preceding claims, arranged such that if said restart signal has been generated a predetermined number of times, then, in case an error occurs again, said stop signal is generated.

12. A computer device according to any of the preceding claims, comprising a switching member (24) for manually generating said restart signal.

13. A computer device arranged to secure the normal function of the computer device under the execution of at least one application program also when an error occurs that normally leads to disconnection and shut-off of the computer device or at least to disconnection concerning said application program, which computer device comprises

processor means (10), an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least an application program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs in the execution of at least said application program, send a restart signal or a stop signal to the processor means (10),

characterised by

a further memory unit (16) that is arranged to comprise at least some basic application instructions, wherein the computer device is arranged such that always when a restart takes place in response to a restart signal generated by the supervisory unit (14), the processor means (10) is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10), wherein the computer device is arranged such that the execution of the application that is controlled by said application program may continue on the basis of the application instructions that are retrieved from the further memory unit, wherein the execution of the application in question may continue without the necessity for the computer device to be disconnected.

14. A method for securing the normal function of a computer device under the execution of at least one application program also when an error occurs that normally leads to disconnection and shut-off of the computer device or at least to disconnection concerning said application program, which computer device comprises

processor means (10),

an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least one application program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs in the execution of at least said application program, send a restart signal or a stop signal to the processor means (10),

a further memory unit (16) that is arranged to comprise at least some basic application instructions,

which method comprises that always when a restart takes place in response to a restart signal generated by the supervisory unit (14), the processor means (10) is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10), wherein the execution of the application that is controlled by said application program may continue on the basis of the application instructions that are retrieved from the further memory unit such that the execution of the application in question may continue without the necessity for the computer device to be disconnected.

15. Use of a computer device according to any of the preceding claims for controlling a system that is included in an aircraft.

RECORD COPY

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No. PCT/SE 0 0 / 0 1 8 4 7

International Filing Date 2 2 -09- 2000

The Swedish Patent Office
PCT International Application

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 55001 PCT si/lt

Box No. I TITLE OF INVENTION

"A computer device with a safety function"

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

SAAB AB
SE-581 88 Linköping
SWEDEN

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: Sweden

State *(that is, country)* of residence: Sweden

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

ALMESÅKER, Marieanne
Ekkällegatan 3
SE-582 30 Linköping
SWEDEN

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: Sweden

State *(that is, country)* of residence: Sweden

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

BJERKENS PATENTBYRÅ KB, represented by
BERGLUND, Stefan; ISRAELSSON, Stefan;
BJERKÉN, Håkan or OLSSON, Jan

Östermalmsgatan 58
SE-114 50 Stockholm, SWEDEN

Telephone No. 08 - 662 08 70

Facsimile No. 08 - 663 02 60

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

NYSTRÖM, Bengt
Dillstigen 6
SE-589 23 Linköping
SWEDEN

This person is:
- [ ] applicant only
- [X] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: Sweden

State *(that is, country)* of residence: Sweden

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [X] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

- [ ] Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No. V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

☒ **AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

☒ **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ **OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☒ **AE** United Arab Emirates
☒ **AG** Antigua and Barbuda
☒ **AL** Albania .....
☒ **AM** Armenia .....
☒ **AT** Austria .....
☒ **AU** Australia .....
☒ **AZ** Azerbaijan
☒ **BA** Bosnia and Herzegovina .....
☒ **BB** Barbados
☒ **BG** Bulgaria .....
☒ **BR** Brazil .....
☒ **BY** Belarus .....
☒ **BZ** Belize
☒ **CA** Canada
☒ **CH** and **LI** Switzerland and Liechtenstein
☒ **CN** China .....
☒ **CR** Costa Rica .....
☒ **CU** Cuba .....
☒ **CZ** Czech Republic and utility model
☒ **DE** Germany and utility model
☒ **DK** Denmark and utility model
☒ **DM** Dominica
☒ **DZ** Algeria .....
☒ **EE** Estonia and utility model
☒ **ES** Spain .....
☒ **FI** Finland and utility model
☒ **GB** United Kingdom
☒ **GD** Grenada
☒ **GE** Georgia .....
☒ **GH** Ghana .....
☒ **GM** Gambia
☒ **HR** Croatia .....
☒ **HU** Hungary .....
☒ **ID** Indonesia
☒ **IL** Israel .....
☒ **IN** India .....
☒ **IS** Iceland
☒ **JP** Japan .....
☒ **KE** Kenya .....
☒ **KG** Kyrgyzstan .....
☒ **KP** Democratic People's Republic of Korea .....
☒ **KR** Republic of Korea .....
☒ **KZ** Kazakhstan .....
☒ **LC** Saint Lucia
☒ **LK** Sri Lanka
☒ **LR** Liberia
☒ **LS** Lesotho .....
☒ **LT** Lithuania
☒ **LU** Luxembourg
☒ **LV** Latvia
☒ **MA** Morocco .....
☒ **MD** Republic of Moldova .....
☒ **MG** Madagascar .....
☒ **MK** The former Yugoslav Republic of Macedonia .....
☒ **MN** Mongolia
☒ **MW** Malawi .....
☒ **MX** Mexico .....
☒ **MZ** Mozambique
☒ **NO** Norway
☒ **NZ** New Zealand .....
☒ **PL** Poland .....
☒ **PT** Portugal .....
☒ **RO** Romania
☒ **RU** Russian Federation .....
☒ **SD** Sudan
☒ **SE** Sweden
☒ **SG** Singapore
☒ **SI** Slovenia .....
☒ **SK** Slovakia and utility model
☒ **SL** Sierra Leone .....
☒ **TJ** Tajikistan .....
☒ **TM** Turkmenistan .....
☒ **TR** Turkey .....
☒ **TT** Trinidad and Tobago .....
☒ **TZ** United Republic of Tanzania
☒ **UA** Ukraine .....
☒ **UG** Uganda .....
☒ **US** United States of America .....
☒ **UZ** Uzbekistan .....
☒ **VN** Viet Nam .....
☒ **YU** Yugoslavia .....
☒ **ZA** South Africa .....
☒ **ZW** Zimbabwe .....

Check-box reserved for designating States which have become party to the PCT after issuance of this sheet:

☐ .....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) 22/09/99	9903422-5	Sweden		
item (2)				
item (3)				

☒ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): (1)

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*: ISA / SE

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date (day/month/year)	Number	Country (or regional Office)
22/05/99 17/05/00	SE99/01277	Sweden

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	4	✓
description (excluding sequence listing part)	11	✓
claims	4	✓
abstract	1	✓
drawings	1	✓
sequence listing part of description		
Total number of sheets	21	

This international application is **accompanied by** the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☒ other *(specify)*: ITS-report

Figure of the drawings which should accompany the abstract: 1

Language of filing of the international application: Swedish

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Stockholm, 22 September 2000
Bjerkéns Patentbyrå KB
Stefan Israelsson

For receiving Office use only

1. Date of actual receipt of the purported international application:	22 -09- 2000	2. Drawings: ☒ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		
4. Date of timely receipt of the required corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA /SE	6. ☐ Transmittal of search copy delayed until search fee is paid.	

For International Bureau use only

Date of receipt of the record copy by the International Bureau: 30 OCTOBER 2000 30 OCT 2000

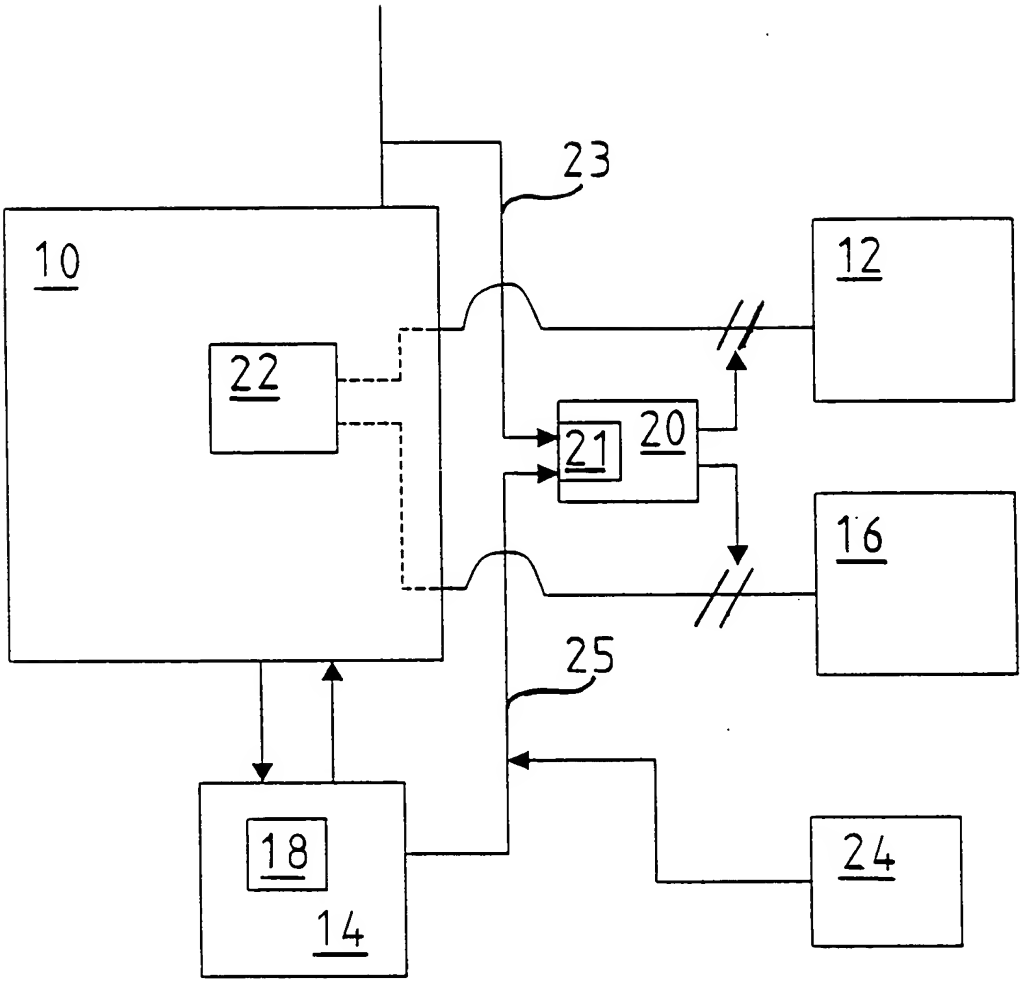


FIG. 1

Datoranordning med säkerhetsfunktion

UPPFINNINGENS BAKGRUND OCH TIDIGARE TEKNIK

Föreliggande uppfinning avser en datoranordning med säkerhetsfunktion för att undvika ej nödvändig nedkoppling av datoranordningen, innefattande processororgan, en ordinarie minnesenhet ansluten till nämnda processororgan och inrättad att innehålla åtminstone ett program som exekveras av processororganet, en övervakningsenhet som övervakar datoranordningens funktion och som är inrättad att, om fel uppstår, sända en återstartsignal eller stoppsignal till processororganet.

Sådana datoranordningar är tidigare kända. Övervakningsenheten kan exempelvis utgöras av en så kallad "watchdog timer". US-A-4 763 296 beskriver funktionen av en sådan watchdog timer. En sådan anordning har således en timer som kontinuerligt är i drift när datoranordningen används. Om timern uppnår ett förutbestämt värde, dvs om en förutbestämd tid har löpt ut, så genererar watchdog-timern en återstartsignal som förorsakar en återstart (reset) av datoranordningen. Under normal användning nollställs timern med jämna mellanrum av processorns normala programförlopp. Om fel skulle uppstå, exempelvis om datorn exekverar en oändlig subrutin, nollställs inte timern och watchdog-timern förorsakar således en omstart av systemet.

Även andra typer av datoranordningar med säkerhetsfunktioner är förut kända. Således beskriver EP-A-481 508 en anordning som innefattar ett backup-minne. När strömförsörjningen stängs av till datoranordningen överförs centralprocessorns status och innehållet i ett huvudminne till nämnda backup-minne. När sedan datoranordningen åter startas genom att strömförsörjningen

ansluts på nytt så återställs vad som finns lagrat i backup-minnet.

EP-A-265 366 beskriver en datoranordning som innefattar ett primärt minne och ett backup-minne. Omkoppling från det primära minnet till backup-minnet görs med hjälp av en "Backup Control System Transfer Mechanism". Denna mekanism är relativt komplicerad. Vid generering av en power-on-reset signal säkerställer nämnda mekanism att omstart sker från primärminnet (se spalt 6, rad 21-28).

Det föreligger ett behov av att förbättra säkerhetsfunktionen hos en datoranordning. Sålunda finns ett behov att på ett säkert sätt omstarta datoranordningen när ett fel har detekterats. Ett sådant fel som kan förorsaka fel i datorns drift är exempelvis minnesfel som kan uppträda i det minne där program finns lagrade som exekveras i datoranordningen. Fel kan även förorsakas av programvaran som finns lagrad i datoranordningens minne. Exempelvis kan sådana fel uppstå om ny programvara används som inte är fullständigt utprovad. Vidare finns ett behov av att säkerställa funktionen hos datoranordningen med relativt enkla medel. Ett ytterligare problem är att säkerställa åtminstone vissa basfunktioner hos datoranordningen när olika fel uppstår.

SAMMANFATTNING AV UPPFINNINGEN

Ändamålet med föreliggande uppfinning är att åstadkomma en datoranordning med en tillförlitlig säkerhetsfunktion som dessutom uppnås med relativt enkla medel.

Detta ändamål uppnås med den inledningsvis angivna datoranordningen som kännetecknas av en ytterligare minnesenhet som är inrättad att innehålla åtminstone vissa grundläggande systeminstruktioner, varvid datoranordningen är inrättad så att processororganet, vid återstart genererad av nämnda återstartsignal från övervakningsenheten, kopplas upp mot den ytterli-

gare minnesenheten och läser och exekverar instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten är bortkopplad från processororganet.

Genom att processororganet kopplas upp mot den ytterligare minnesenheten när en återstartsignal har genererats av övervakningsenheten så undviks att eventuella fel som föreligger i de instruktioner som är lagrade i den ordinarie minnesenheten överförs till processororganet. Därigenom uppnås en säkrare funktion av datoranordningen efter det att en återstartsignal har genererats som svar på ett detekterat fel. I detta sammanhang bör noteras att när i patentkraven och beskrivningen anges att en minnesenhet kopplas upp eller är bortkopplad från processororganet så menas därmed inte nödvändigtvis att bortkoppling sker genom att fysiskt bryta förbindelsen mellan processororganet och minnesenheten i fråga. Begreppen koppla upp och bortkoppla innefattar således två möjligheter: dels fysisk koppling genom brytning av förbindelsen, dels uppkoppling och bortkoppling på programnivå.

Det bör noteras att med begreppet "systeminstruktioner" avses i denna ansökan företrädesvis, men ej nödvändigtvis, program som styr ett system eller en del av ett system som styrs av datoranordningen, dvs begreppet "systeminstruktioner" avser applikationsinstruktioner.

Enligt en utföringsform av uppfinningen utgör den ordinarie minnesenheten och den ytterligare minnesenheten två olika, fysiskt separata, minnen. Därigenom uppnås ökad säkerhet eftersom den ordinarie minnesenheten föreligger som ett separat minne som är helt bortkopplat från processororganet vid återstart.

Enligt en alternativ utföringsform av uppfinningen utgör den ordinarie minnesenheten och den ytterligare minnesenheten två delar av fysiskt samma minne, men med olika minnesadresser. Genom denna konstruktion krävs färre minneskomponenter ef-

tersom den ytterligare minnesenheten finns lagrad som en speciell del av det minne där även den ordinarie minnesenheten ingår.

Enligt en ytterligare utföringsform av uppfinningen är nämnda övervakningsenhet inrättad att generera en signal i beroende av en timer på så sätt att nämnda återstartsignal genereras om ingen trigger-signal som nollställer timern erhålls inom ett förutbestämt tidsintervall. Övervakningsenheten kan i detta fall således utgöras av en så kallad watchdog timer (WDT). En sådan WDT ingår ofta i datoranordningar. Således kan en sådan väl fungerande redan befintlig WDT användas som övervakningsenhet i anordningen enligt föreliggande uppfinning. Det bör dock påpekas att även andra typer av övervakningsenheter än en WDT kan användas i datoranordningen enligt uppfinningen.

Enligt ännu en utföringsform av uppfinningen innefattar datoranordningen en minnessäkerhetskrets som är inrättad att stoppa inläsning från den ordinarie minnesenheten och att koppla upp för inläsning från nämnda ytterligare minnesenhet när både nämnda återstartsignal och en signal indikerande pålagd drivspänning föreligger. En sådan minnessäkerhetskrets är en relativt enkel och väl fungerande krets som tillser att omkoppling från den ordinarie till den ytterligare minnesenheten sker. Vidare säkerställer denna minnessäkerhetskrets att en sådan omkoppling endast sker om drivspänning till datoranordningen föreligger.

Enligt en ytterligare utföringsform av uppfinningen är nämnda ytterligare minnesenhet inrättad så att den innehåller grundläggande systeminstruktioner men en hög nivå av funktionssäkerhet. Den ytterligare minnesenheten kan härvid vara inrättad att innehålla systeminstruktioner som redan har varit väl testade och som därför har en hög funktionssäkerhet. Den ytterligare minnesenheten kan härvid också vara försedd med de grundläggande instruktionerna för datoranordningen medan icke nöd-

vändiga systeminstruktioner har uteslutits från nämnda ytterligare minnesenhet.

Enligt ännu en utföringsform av uppfinningen är nämnda ytterligare minnesenhet inrättad så att den innehåller systeminstruktioner med en nivå av funktionssäkerhet som är högre än den nivå av funktionssäkerhet som föreligger i den ordinarie minnesenheten. Således kan den ordinarie minnesenheten innefatta systeminstruktioner som ej är så väl testade i datoranordningen. Den ytterligare minnesenheten kan därvid innehålla de grundläggande systeminstruktionerna som redan har visat sig ha hög funktionssäkerhet. Inom uppfinningens ram ligger givetvis även möjligheten att den ordinarie minnesenheten och den ytterligare minnesenheten innehåller systeminstruktioner med samma nivå av funktionssäkerhet.

Enligt en ytterligare utföringsform av uppfinningen är åtminstone nämnda ytterligare minnesenhet ett icke flyktigt minne. Detta bidrar till en ökad funktionssäkerhet hos datoranordningen.

Enligt ännu en utföringsform av uppfinningen innefattar nämnda processororgan ett arbetsminne som är så inrättat att vid återstart av datoranordningen nollställs detta arbetsminne innan inläsning från nämnda ytterligare minnesenhet påbörjas. Därigenom säkerställs att instruktioner som kan innehålla fel och som härrör från den ordinarie minnesenheten ej kvarligger i arbetsminnet innan inläsning från den ytterligare minnesenheten påbörjas.

Enligt en ytterligare utföringsform av uppfinningen är nämnda ytterligare minnesenhet inrättad att vara skrivskyddad åtminstone då datoranordningen är i drift. Detta bidrar till ytterligare säkerhet eftersom innehållet i den ytterligare minnesenheten är skyddat och ej kan ändras då datoranordningen är i drift.

Enligt ännu en utföringsform av uppfinningen är datoranordningen inrättad så att om nämnda återstartsignal har genererats ett förutbestämt antal gånger så genereras, om åter ett fel uppstår, nämnda stoppsignal. Detta innebär att övervakningsenheten genererar ett förutbestämt antal återstartsignaler. Om det visar sig att fel föreligger även efter det att ett förutbestämt antal återstartförsök har gjorts så stoppas datoranordningen.

Enligt ännu en utföringsform av uppfinningen innefattar datoranordningen omkopplingsorgan för att manuellt generera nämnda återstartsignal. Detta innebär att förutom automatisk generering av återstartsignal genom övervakningsenheten kan även en manuell återstartsignal genereras av en operatör. En operatör kan således beordra att återstart från den ytterligare minnesenheten ska ske.

En ytterligare utföringsform av uppfinningen framgår av patentkrav 13. Denna utföringsform kan även kombineras med särdragen hos ett eller flera av patentkraven 2-12.

Uppfinningens ändamål uppnås även med en metod enligt krav 14. Denna metod har fördelar motsvarande de som beskrivs i samband med anordningen. Metoden enligt krav 14 kan även kombineras med särdrag motsvarande dem som definieras i ett eller flera av patentkraven 2-12.

En föredragen användning av datoranordningen är att använda den för att styra ett system som ingår i olika farkoster exempelvis i luftfartyg. En flygfarkost har många olika funktioner som styrs av en datoranordning. Det är viktigt att dessa funktioner fungerar och att onödig nedkoppling av datoranordningen eller av dess drift beträffande någon applikation undviks. Detta syfte uppnås genom en användning enligt krav 15.

KORT BESKRIVNING AV RITNINGEN

Föreliggande uppfinning skall nu förklaras med hjälp av en beskriven utföringsform, som utgör ett exempel på uppfinningen, och med hänvisning till den bifogade ritningen.

Fig 1 visar schematiskt ett blockschema av en utföringsform av uppfinningen.

DETALJERAD BESKRIVNING AV EN UTFÖRINGSFORM AV UPPFINNINGEN

Fig 1 visar ett blockschema av en utföringsform av uppfinningen. Datoranordningen innefattar ett processororgan 10. Med detta processororgan 10 avses inte endast datoranordningens centrala processorenhet (CPU) utan även andra centrala delar av datoranordningen såsom exempelvis arbetsminnet 22. Datoranordningen innefattar även en ordinarie minnesenhet 12. Denna ordinarie minnesenhet 12 kan exempelvis utgöras av någon form av PROM, exempelvis UVPROM, EEPROM eller liknande. När datoranordningen först startas uppkopplas processororganet 10 mot den ordinarie minnesenheten 12. Denna ordinarie minnesenhet 12 är således inrättad att innehålla de instruktioner som styr datoranordningens drift. Datoranordningen innefattar även en övervakningsenhet 14. Övervakningsenheten 14 övervakar datoranordningens funktion och är inrättad att generera en återstartsignal eller stoppsignal till processororganet 10 om övervakningsenheten 14 detekterar ett fel. Övervakningsenheten 14 kan exempelvis utgöras av en så kallad watchdog timer (WDT). En sådan WDT 14 genererar en signal som beror av en timer 18. En återstartsignal genereras därvid om WDT:n 14 inom ett förutbestämt tidsintervall inte erhåller en trigger-signal som nollställer timern 18. För att ha hög säkerhet innefattar WDT:n 14 lämpligen en egen timer 18. Det är dock möjligt att WDT:ns 14 timer-funktion styrs av samma klocka som ingår i processororganet 10.

Datoranordningen innefattar även en ytterligare minnesenhet 16. Denna ytterligare minnesenhet 16 är inrättad att innehålla åtminstone vissa grundläggande systeminstruktioner. Den ytterligare minnesenheten 16 kan utgöra ett minne som är fysiskt separat från den ordinarie minnesenheten 12. Det är även möjligt att den ordinarie minnesenheten 12 och den ytterligare minnesenheten 16 utgör två delar av fysiskt samma minne. För att ytterligare öka säkerheten om ett minnesfel skulle uppstå kan den ordinarie minnesenheten 12 och den ytterligare minnesenheten 16 utgöras av fysiskt separata minnen av olika typ, exempelvis från olika tillverkare. Den ytterligare minnesenheten utgörs lämpligen av någon form av PROM, exempelvis UVPROM eller EEPROM.

Datoranordningen innefattar även en minnessäkerhetskrets 20. Denna minnessäkerhetskrets 20 kan ingå som en del av processororganet 10. I den visade utföringsformen utgör emellertid minnessäkerhetskretsen 20 en separat krets. Minnessäkerhetskretsen 20 innefattar en AND-grind 21. Minnessäkerhetskretsen 20 styr vilken av den ordinarie minnesenheten 12 och den ytterligare minnesenheten 16 som skall vara inkopplad till processororganet 10. Denna styrning kan antingen utgöras av brytning eller slutning av den elektriska förbindelsen mellan respektive minnesenhet 12, 16 och processorenheten 10 eller också utgöras av styrning på programnivå av dessa förbindelser. Det är även möjligt att styrningen utgörs av en kombination av programvaruinstruktioner och fysisk brytning eller slutning. AND-grindens ena ingång är ansluten till en ledning 23 som indikerar att drivspänning föreligger. AND-grindens 21 andra ingång är ansluten till en ledning 25 som är förbunden med WDT:n 14. Via denna ledning 25 leds en av WDT:n 14 genererad återstartsignal till AND-grinden 21 och därmed till minnessäkerhetskretsen 20.

Datoranordningen innefattar även ett omkopplingsorgan 24 för att manuellt generera en återstartsignal. Detta omkopplingsor-

gan 24 kan lämpligen vara anslutet till den ingång hos AND-grinden som även är ansluten till WDT:n 14.

WDT:n 14 övervakar således datoranordningens funktion. När datoranordningen fungerar normalt erhåller WDT:n 14 med jämna mellanrum en trigger-signal från processororganet 10. Denna trigger-signal nollställer timern 18. Därvid genererar WDT:n 14 ingen återstartsignal till ledningen 25. Om emellertid fel uppstår så att WDT:n 14 ej erhåller någon trigger-signal inom ett förutbestämt tidsintervall från processororganet 10 så genererar WDT:n 14 en återstartsignal. Denna återstartsignal leds således till den ena ingången hos AND-grinden 21. När AND-grinden 21 erhåller en sådan återstartsignal, och om samtidigt AND-grindens 21 andra ingång detekterar att drivspänning föreligger, så tillser minnessäkerhetskretsen 20 att den ordinarie minnesenheten 12 kopplas bort från processororganet 10 och att den ytterligare minnesenheten 16 kopplas upp mot processororganet 10. Även processororganet 10 erhåller en signal, lämpligen från WDT:n 14, om att återstart skall genomföras. Processororganets 10 arbetsminne 22 nollställs därvid, varefter inläsning från den ytterligare minnesenheten 16 sker. Inläsning sker därvid till förutbestämda adresser hos arbetsminnet 22. Processororganet 10 läser och exekverar således de instruktioner som finns lagrade i den ytterligare minnesenheten 16.

Det är tänkbart att ett återstartförsök misslyckas och att WDT:n 14 därför genererar en ny återstartsignal. Om ånyo fel detekteras kan ytterligare återstartsignaler genereras av WDT:n 14. Datoranordningen är därvid lämpligen inrättad så att när ett förutbestämt antal återstartförsök har gjorts så stoppas återstartförsöken. Därvid kan en varningsfunktion genereras av datoranordningen och senaste information beträffande processororganets 10 och minnesenheternas 12, 16 status kan registreras för senare analys. Lämpligen är datoranordningen inrättad så att återstartförsöken stoppas efter exempelvis ett till fyra återstartförsök, företrädesvis efter två återstartförsök. Datoranordningen

kan därvid vara inrättad så att återstartförsöken stoppas om nämnda förutbestämda antal återstartförsök har genomförts inom ett förutbestämt tidsintervall.

För ökad säkerhet är lämpligen den ytterligare minnesenheten 16 inrättad så att den är skrivskyddad när datoranordningen är i drift. Vidare utgörs lämpligen såväl den ordinarie minnesenheten 12 som den ytterligare minnesenheten 16 av icke flyktiga minnen.

Den ytterligare minnesenheten 16 är lämpligen inrättad så att den innehåller grundläggande systeminstruktioner vid en hög nivå av funktionssäkerhet. Den ytterligare minnesenheten 16 kan därvid innehålla primära och välutprovade systemfunktioner. Lämpligen är den ytterligare minnesenheten 16 inrättad så att den därvid innehåller systeminstruktioner med en högre nivå av funktionssäkerhet än de systeminstruktioner som föreligger i den ordinarie minnesenheten 12. Med uttrycket "nivå av funktionssäkerhet" kan härvid exempelvis avses de programvarusäkerhetsnivåer som definierats enligt RTCA-standard dokument NO.RTCA/DO-178B.

Datoranordning enligt uppfinningen kan företrädesvis vara inrättad för att säkerställa normalfunktionen hos datoranordningen under exekvering ett applikationsprogram även när ett fel uppträder som annars skulle leda till nedkoppling och avstängning av datoranordningen, eller åtminstone till att exekveringen av applikationsprogrammet i fråga avbryts. Den ordinarie minnesenheten 12 innehåller således ett applikationsprogram som exekveras av processororganet 10. Om fel uppstår i exekveringen av åtminstone nämnda applikationsprogram kopplas processororganet 10 upp mot den en ytterligare minnesenheten 16 som är inrättad att innehålla åtminstone vissa grundläggande, redan tidigare använda och säkra applikationsinstruktioner. Datoranordningen är således inrättad så att exekveringen av applikationen som styrs av applikations-

programmet kan fortsätta på basis av de applikationsinstruktioner som hämtats från den ytterligare minnesenheten.

Enligt en metod enligt uppfinningen sker, om fel uppstår, uppkoppling mot den ytterligare minnesenheten 16 som innehåller åtminstone vissa grundläggande applikationsinstruktioner. Därigenom kan exekveringen av applikationen som styrs av ett applikationsprogram fortsätta på basis av de applikationsinstruktioner som hämtats från den ytterligare minnesenheten och som inläses på ett normalt och traditionellt sätt till processororganet 10 med normal nollställning av arbetsminnet 22.

Datoranordningen enligt uppfinningen kan med fördel användas för att styra ett system som ingår i en flygfarkost.

Föreliggande uppfinning är inte begränsad till den visade utföringsformen utan kan varieras och modifieras inom ramen för de efterföljande patentkraven.

Patentkrav

1. Datoranordning med säkerhetsfunktion för att undvika ej nödvändig nedkoppling av datoranordningen, innefattande

processororgan (10),

en ordinarie minnesenhet (12) ansluten till nämnda processororgan (10) och inrättad att innehålla åtminstone ett program som exekveras av processororganet (10),

en övervakningsenhet (14) som övervakar datoranordningens funktion och som är inrättad att, om fel uppstår, sända en återstartsignal eller stoppsignal till processororganet (10),

kännetecknad av

en ytterligare minnesenhet (16) som är inrättad att innehålla åtminstone vissa grundläggande systeminstruktioner, varvid datoranordningen är inrättad så att processororganet (10), vid återstart genererad av nämnda återstartsignal från övervakningsenheten (14), kopplas upp mot den ytterligare minnesenheten (16) och läser och exekverar instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten (12) är bortkopplad från processororganet (10).

2. Datoranordning enligt krav 1, varvid den ordinarie minnesenheten (12) och den ytterligare minnesenheten (16) utgör två olika, fysiskt separata, minnen.

3. Datoranordning enligt krav 1, varvid den ordinarie minnesenheten (12) och den ytterligare minnesenheten (16) utgör två delar av fysiskt samma minne, men med olika minnesadresser.

4. Datoranordning enligt något av föregående krav, varvid nämnda övervakningsenhet (14) är inrättad att generera en signal i beroende av en timer (18) på så sätt att nämnda återstartsignal genereras om ingen trigger-signal signal som nollställer timern (18) erhålls inom ett förutbestämt tidsintervall.

5. Datoranordning enligt något av föregående krav, innefattande en minnessäkerhetskrets (20) som är inrättad att stoppa inläsning från den ordinarie minnesenheten (12) och att koppla upp för inläsning från nämnda ytterligare minnesenhet (16) när både nämnda återstartsignal och en signal indikerande pålagd drivspänning föreligger.

6. Datoranordning enligt något av föregående krav, varvid nämnda ytterligare minnesenhet (16) är inrättad så att den innehåller grundläggande systeminstruktioner med en hög nivå av funktionssäkerhet.

7. Datoranordning enligt krav 6, varvid nämnda ytterligare minnesenhet (16) är inrättad så att den innehåller systeminstruktioner men en nivå av funktionssäkerhet som är högre än den nivå av funktionssäkerhet som föreligger i den ordinarie minnesenheten (12).

8. Datoranordning enligt något av föregående krav, varvid åtminstone nämnda ytterligare minnesenhet (16) är ett icke flyktigt minne.

9. Datoranordning enligt något av föregående krav, varvid nämnda processororgan (10) innefattar ett arbetsminne (22) som är så inrättat att vid återstart av datoranordningen nollställs detta arbetsminne (22) innan inläsning från nämnda ytterligare minnesenhet (16) påbörjas.

10. Datoranordning enligt något av föregående krav, varvid nämnda ytterligare minnesenhet (16) är inrättad att vara skrivskyddad åtminstone då datoranordningen är i drift.

11. Datoranordning enligt något av föregående patentkrav, inrättad så att om nämnda återstartsignal har genererats ett förutbestämt antal gånger så genereras, om åter ett fel uppstår, nämnda stoppsignal.

12. Datoranordning enligt något av föregående krav, innefattande omkopplingsorgan (24) för att manuellt generera nämnda återstartsignal.

13. Datoranordning inrättad för att säkerställa normalfunktionen hos datoranordningen under exekvering av åtminstone ett applikationsprogram även när ett fel uppträder som normalt leder till nedkoppling och avstängning av datoranordningen eller åtminstone nedkoppling vad avser nämnda applikationsprogram, vilken datoranordning innefattar

processororgan (10),

en ordinarie minnesenhet (12) ansluten till nämnda processororgan (10) och inrättad att innehålla åtminstone ett applikationsprogram som exekveras av processororganet (10),

en övervakningsenhet (14) som övervakar datoranordningens funktion och som är inrättad att, om fel uppstår i exekveringen av åtminstone nämnda applikationsprogram sända en återstartsignal eller stoppsignal till processororganet (10),

<u>kännetecknad av</u>

en ytterligare minnesenhet (16) som är inrättad att innehålla åtminstone vissa grundläggande applikationsinstruktioner, varvid datoranordningen är inrättad så att alltid när återstart sker som svar på en återstartsignal genererad av övervakningsenheten (14), processororganet (10) kopplas upp mot den ytterligare minnesenheten (16) och läser och exekverar instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten (12) är bortkopplad från processororganet (10), varvid datoranordningen är inrättad så att exekveringen av applikationen som styrs av nämnda applikationsprogram kan fortsätta på basis av de applikationsinstruktioner som hämtats från den ytterligare minnesenheten, varvid exekveringen av applikationen i fråga kan fortsätta utan att datoranordningen behöver kopplas ned.

14. En metod för att säkerställa normalfunktionen hos en datoranordningen under exekvering av åtminstone ett applikationsprogram även när ett fel uppträder som normalt leder till nedkoppling och avstängning av datoranordningen eller åtminstone nedkoppling vad avser nämnda applikationsprogram, vilken datoranordning innefattar

processororgan (10),

en ordinarie minnesenhet (12) ansluten till nämnda processororgan (10) och inrättad att innehålla åtminstone ett applikationsprogram som exekveras av processororganet (10),

en övervakningsenhet (14) som övervakar datoranordningens funktion och som är inrättad att, om fel uppstår i exekveringen av åtminstone nämnda applikationsprogram sända en återstartsignal eller stoppsignal till processororganet (10),

en ytterligare minnesenhet (16) som är inrättad att innehålla åtminstone vissa grundläggande applikationsinstruktioner,

vilken metod innefattar att alltid när återstart sker som svar på en återstartsignal genererad av övervakningsenheten (14), så kopplas processororganet (10) upp mot den ytterligare minnesenheten (16) och läser och exekverar instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten (12) är bortkopplad från processororganet (10), varigenom exekveringen av applikationen som styrs av nämnda applikationsprogram kan fortsätta på basis av de applikationsinstruktioner som hämtats från den ytterligare minnesenheten så att exekveringen av applikationen i fråga kan fortsätta utan att datoranordningen behöver kopplas ned

15. Användning av en datoranordning enligt något av föregående krav för att styra ett system som ingår i en flygfarkost.

Sammandrag

Uppfinningen avser en datoranordning med säkerhetsfunktion för att undvika ej nödvändig nedkoppling av datoranordningen. Datoranordningen innefattar processororgan (10), en ordinarie minnesenhet (12), en övervakningsenhet (14) och en ytterligare minnesenhet (16). Datoranordningen är inrättad så att processororganet (10) vid en återstart genererad av en återstartsignal, kopplas upp mot den ytterligare minnesenheten (16) och läser och exekverar de instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten (12) är bortkopplad från processororganet (10).

(Fig 1)

Amended

Claims

1. A computer device with a safety function for avoiding non necessary disconnection of the computer device, comprising

processor means (10),

an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least one program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs, send a restart signal or a stop signal to the processor means (10),

characterised by

a further memory unit (16) that is arranged to comprise at least some basic system instructions, wherein the computer device is arranged such that the processor means (10), at a restart generated by said restart signal from the supervisory unit (14), is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10).

2. A computer device according to claim 1, wherein the ordinary memory unit (12) and the further memory unit (16) constitute two different, physically separate, memories.

3. A computer device according to claim 1, wherein the ordinary memory unit (12) and the further memory unit (16) constitute two parts of physically the same memory, but with different memory addresses.

4. A computer device according to any of the preceding claims, wherein said supervisory unit (14) is arranged to generate a signal in dependence of a timer (18) in such a manner that said restart signal is generated if no trigger-signal signal that sets the timer (18) to zero is received within a predetermined time interval.

5. A computer device according to any of the preceding claims, comprising a memory safety circuit (20) that is arranged to stop the

reading from the ordinary memory unit (12) and to connect for reading from said further memory unit (16) when both said restart signal and a signal indicating applied supply voltage is the case.

6. A computer device according to any of the preceding claims, wherein said further memory unit (16) is arranged such that it comprises basic system instructions with a high degree of reliability.

7. A computer device according to claim 6, wherein said further memory unit (16) is arranged such that it comprises system instructions with a degree of reliability that is higher than the degree of reliability that is the case in the ordinary memory unit (12).

8. A computer device according to any of the preceding claims, wherein at least said further memory unit (16) is a non-volatile memory.

9. A computer device according to any of the preceding claims, wherein said processor means (10) comprises a working memory (22) that is arranged such that at a restart of the computer device this working memory (22) is reset before reading from said further memory unit (16) is started.

10. A computer device according to any of the preceding claims, wherein said further memory unit (16) is arranged to be write protected at least when the computer device is in operation.

11. A computer device according to any of the preceding claims, arranged such that if said restart signal has been generated a predetermined number of times, then, in case an error occurs again, said stop signal is generated.

12. A computer device according to any of the preceding claims, comprising a switching member (24) for manually generating said restart signal.

13. A computer device arranged to secure the normal function of the computer device under the execution of at least one application program also when an error occurs that normally leads to disconnection and shut-off of the computer device or at least to disconnection concerning said application program, which computer device comprises

processor means (10), an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least an application program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs in the execution of at least said application program, send a restart signal or a stop signal to the processor means (10),

characterised by

a further memory unit (16) that is arranged to comprise at least some basic application instructions, wherein the computer device is arranged such that always when a restart takes place in response to a restart signal generated by the supervisory unit (14), the processor means (10) is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10), wherein the computer device is arranged such that the execution of the application that is controlled by said application program may continue on the basis of the application instructions that are retrieved from the further memory unit, wherein the execution of the application in question may continue without the necessity for the computer device to be disconnected.

14. A method for securing the normal function of a computer device under the execution of at least one application program also when an error occurs that normally leads to disconnection and shut-off of the computer device or at least to disconnection concerning said application program, which computer device comprises

processor means (10),

an ordinary memory unit (12) connected to said processor means (10) and arranged to comprise at least one application program that is executed by the processor means (10),

a supervisory unit (14) that supervises the function of the computer device and that is arranged to, in case an error occurs in the execution of at least said application program, send a restart signal or a stop signal to the processor means (10),

a further memory unit (16) that is arranged to comprise at least some basic application instructions,

which method comprises that always when a restart takes place in response to a restart signal generated by the supervisory unit (14), the processor means (10) is connected to the further memory unit (16) and reads and executes instructions that are stored in the same, while the ordinary memory unit (12) is disconnected from the processor means (10), wherein the execution of the application that is controlled by said application program may continue on the basis of the application instructions that are retrieved from the further memory unit such that the execution of the application in question may continue without the necessity for the computer device to be disconnected.

15. Use of a computer device according to any of the preceding claims for controlling a system that is included in an aircraft.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01847

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 9/445, G06F 11/00, G06F 11/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9908186 A1 (A. SUN ET AL), 18 February 1999 (18.02.99), page 3, line 19 - line 23; page 6, line 11 - line 17; page 7, line 8 - line 20, page 8, line 5 - line 13; page 9, line 2 - line 11; claims 22 - 24	1-15
	--	
X	US 5247659 A (M. CURRAN ET AL), 21 Sept 1993 (21.09.93), column 1, line 35 - line 54, claim 1, abstract	1-15
	--	
X	US 5432927 A (J. GROTE ET AL), 11 July 1995 (11.07.95), column 2, line 51 - column 3, line 22, abstract	1-15
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December 2000	27 -12- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Pär Heimdal/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01847

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4491914 A (J. SUJAKO), 1 January 1985 (01.01.85), column 1, line 65 - column 2, line 22 -- --------	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 00/01847

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9908186 A1	18/02/99	EP 1008042 A	14/06/00
US 5247659 A	21/09/93	AU 621405 B	12/03/92
		AU 4253589 A	12/04/90
		DE 68910075 D,T	19/05/94
		EP 0364127 A,B	18/04/90
		GB 8823509 D	00/00/00
		ZA 8907359 A	25/07/90
US 5432927 A	11/07/95	NONE	
US 4491914 A	01/01/85	JP 58097724 A	10/06/83
		JP 61014542 B	19/04/86
		KR 8600810 B	28/06/86